UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Records and information associated with the cellular device assigned IP Address 2607:fb90:d258:b79e:2b93:990b:99fb:033c, whose service provider is T-Mobile US, Inc., a wireless telephone service provider headquartered at 4 Sylvan, Parsippany, NJ 07054, utilized on March 18, 2022 multiple times that are more fully described in Attachment A.

Case No. 22 MJ 52

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1951(a); 18 U.S.C. § 924(c); 18 U.S.C. §§ 922(g)(1) and 924(a)(2)	Hobbs Act Robbery; brandishing a firearm during a crime of violence; and felon in possession of a firearm.

The application is based on these facts:

See attached Affidavit.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days: _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

David Bianchi, SA FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 3/21/2022

Judge's signature

City and state: Milwaukee, WI

Hon. William E. Duffin, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent David Bianchi, being first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A), for information about the location of the cellular telephone assigned IP Address: 2607:fb90:d258:b79e:2b93:990b:99fb:033c, which was utilized multiple times listed in Attachment A on March 18, 2022 (the "Target Cell Phone"), whose service provider is **T-Mobile US, Inc.** ("Service Provider"), a wireless telephone service provider headquartered at 4 Sylvan, Parsippany, NJ 07054. The Target Cell Phone is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

2. Because this warrant application seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a "pen register" and/or "trap and trace device," *see* 18 U.S.C. § 3127(3) & (4), I also make this affidavit in support of an application by the United States of America for an order pursuant to 18 U.S.C §§ 3122 and 3123, authorizing the installation and use of pen registers and trap and trace devices ("pen-trap devices") to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from the Target Cell Phone.

3. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since January 2020. Since September 2020, I have been assigned to the FBI's Milwaukee Area Violent Crimes Task Force. This Task Force is a multi-jurisdictional law enforcement entity charged with investigating violations of federal law, including bank robberies, commercial robberies and other violent crime matters, defined under Title 18 of the United States Code. I

have been trained in a variety of investigative and legal matters, including the topics of Fourth Amendment searches, the drafting of search warrant affidavits, and probable cause. I have assisted in criminal investigations, participating in surveillance, interviews, and debriefs of arrested subjects. As a result of this training and investigative experience, I have learned how and why violent actors typically conduct various aspects of their criminal activities.

4. The facts in this affidavit come from my training, experience and information provided to me by other Law Enforcement Officers, my review of documents and information obtained from other agents. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that Antonio D. MOORE has violated 18 U.S.C. § 1951(a) (Hobbs Act Robbery) and 18 U.S.C. § 924(c) (Brandishing a Firearm During a Crime of Violence) in the State and Eastern District of Wisconsin.

6. On March 3, 2022, a criminal complaint was issued in the Eastern District of Wisconsin, charging Antonio D. MOORE, DOB XX/XX/1992, with one count of Hobbs Act Robbery, one count of Brandishing a Firearm During a Crime of Violence, and one count of Possession of a Firearm by a Convicted Felon, in violation of 18 U.S.C. §§ 1951(a), 924(c), and 922(g)(1). An arrest warrant for MOORE was issued the same day.

7. There is also probable cause to believe that the information described in Attachment B will assist law enforcement in arresting MOORE, who is a "person to be arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

JURISDICTION

8. The court has jurisdiction to issue the proposed warrant because it is a "court of

competent jurisdiction" as defined 18 U.S.C. Section 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. Section 2711(3)(A)(i).

PROBABLE CAUSE

9. On March 3, 2022, this affiant conducted an open-source Facebook query of MOORE's known associates. This affiant identified the Facebook page of MOORE's mother, E.T., which returned to the account: facebook.com/elva.thomas.90. A publicly viewable search of E.T.'s Facebook posts showed that an individual with the Facebook username "Solo Elevated" "liked" a post from February 10, 2022. The page "Solo Elevated" returned to the account: facebook.com/100008737363815. The Facebook User ID associated with this account is: 100008737363815. The Affiant did observe Facebook posts on February 10, 2022, but also knows that not all Facebook content is visible unless you are Facebook friends and knows you can use the private messenger, so only the people you are communicating with can see the conversation. The publicly viewable "profile picture" associated with this account matched the known photographs of MOORE which were previously located in various law enforcement databases.

10. On March 11, 2022, United States Magistrate, Judge William E. Duffin, Eastern District of Wisconsin, authorized a pen register trap and trace for the identified Facebook account; https://www.facebook.com/100008737363815, Facebook ID # "100008737363815", for MOORE.

11. Results of the on-going pen register trap and trace of Facebook account, https://www.facebook.com/100008737363815, show that between the dates of March 11, 2022, and March 20, 2022, log-in IP addresses for the account have appeared and verified that

MOORE has been utilizing his account. Identified IP addresses show that there is consistent usage of a T-Mobile device. The most recent IP Address is shown to be 2607:fb90:d25f:f2cc:44b4:1799:4dff:5f9c, utilized 2022-03-20 15:19:55 UTC (the "Target Cell Phone"), whose service provider is T-Mobile ("Service Provider"), a wireless telephone service provider headquartered at 4 Sylvan, Parsippany, NJ 07054.

12. I believe that by obtaining the information described in Attachments A and B, law enforcement will be able to locate MOORE and arrest him on the outstanding warrant.

13. The affiant knows that subjects who are wanted for crimes and are trying to remain "at large" use social media frequently to communicate with family/friends/co-actors. It is common for wanted subjects to set these social media accounts to "Private" or lock the access to them, use alias names, and use accounts of other persons to remain undetected by law enforcement authorities.

TECHNICAL BACKGROUND: DYNAMIC IP ADDRESSES

14. Your affiant utilized the website www.arin.net, the "American Registry of Internet Numbers (ARIN)," to obtain the owner and operator of the IP address mentioned previously: 2607:fb90:d258:b79e:2b93:990b:99fb:033c, which was utilized multiple times listed in Attachment A on March 18, 2022. According to ARIN, the listed IP address is owned and operation by **T-Mobile**. Your affiant has utilized ARIN in the past and knows this website to be reliable.

15. Based on training, experience and information provided to me by other Law Enforcement Officers, I know that **T-Mobile** is a cellular service provider and does have the ability to connect their cellular service to the internet through Dynamic Internet Protocols. A dynamic Internet Protocol address (dynamic IP address) is a temporary IP address that is

assigned to a computing device or node when it's connected to a network. A dynamic IP address is an automatically configured IP address assigned by a Dynamic Host Configuration Protocol (DHCP) server to every new network node.

16. Dynamic IP addresses are generally implemented by Internet service providers and networks that have a large number of connecting clients or end-nodes. Unlike static IP addresses, dynamic IP addresses are not permanent. A dynamic IP is assigned to a node until it's connected to the network; therefore, the same node may have a different IP address every time it reconnects with the network.

17. I know through training, experience and information provided to me by other Law Enforcement Officers that **T-Mobile** is able to "resolve" associated Dynamic IP addresses. When **T-Mobile** "resolves" those IP addresses, they are able to identify the associated user and the specific cellular phone associated with that user. In other words, when **T-Mobile** is provided with a particular associated IP address and time stamp (like the IP address and time stamp described here), **T-Mobile** is able to (i) determine the particular cellular phone that utilized that IP address; and (ii) collect cell-site location data associated with that same particular cellular phone, in the manner described below.

TECHNICAL BACKGROUND: CELL SITE LOCATION DATA

18. In my training, experience and information provided to me by other Law Enforcement Officers, I have learned that the Service Provider is a company that provides cellular communications service to the general public. I also know that providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site

data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the "sector" (i.e., faces of the towers) to which the device connected. These towers are often a half- mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate general location of the cellular device.

19. Based on my training, experience and information provided to me by other Law Enforcement Officers, I know that the Service Provider can collect cell-site data on a prospective basis about the Target Cell Phone. Based on my training, experience and information provided to me by other Law Enforcement Officers, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer was connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as the Service Provider typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

20. I know that some providers of cellular telephone service have technical capabilities that allow them to collect and generate E-911 Phase II data, also known as GPS data or latitude-longitude data. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. As discussed above, cell-site data identifies the "cell towers" (i.e., antenna towers covering specific

geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise that E-911 Phase II data. Based on my training, experience and information provided to me by other Law Enforcement Officers, I know that the Service Provider can collect E-911 Phase II data about the location of the Target Cell Phone, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available.

21. Based on my training, experience and information provided to me by other Law Enforcement Officers, I know each cellular device has one or more unique identifiers embedded inside it. Depending on the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), a Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Equipment Identity ("IMEI"). The unique identifiers – as transmitted from a cellular device to a cellular antenna or tower – can be recorded by pen-trap devices and indicate the identity of the cellular device making the communication without revealing the communication's content.

22. Based on my training, experience and information provided to me by other Law

Enforcement Officers, I know that wireless providers such as the Service Provider typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless communication service. I also know that wireless providers such as the Service Provider typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular device and other transactional records, in their normal course of business. In my training, experience and information provided to me by other Law Enforcement Officers, this information may constitute evidence of the crimes under investigation because the information can be used to identify the Target Cell Phone's user or users and may assist in the identification of co-conspirators and/or victims.

23. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

24. I further request that the Court direct the Service Provider to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control.

25. I also request that the Court direct the Service Provider to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with the Service Provider's services, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The

government shall reasonably compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

26. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the Target Cell Phone would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

27. Because the warrant will be served on the Service Provider, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the Target Cell Phone outside of daytime hours.

ATTACHMENT A

Property to Be Searched

Records and information associated with the cellular device assigned IP Address 2607:fb90:d258:b79e:2b93:990b:99fb:033c, utilized at the following dates and times:

- 2022-03-18 01:19:17 UTC
- 2022-03-18 01:19:12 UTC
- 2022-03-18 01:19:03 UTC
- 2022-03-18 01:18:58 UTC
- 2022-03-18 01:12:46 UTC
- 2022-03-18 01:05:21 UTC
- 2022-03-18 01:31:21 UTC
- 2022-03-18 01:31:16 UTC
- 2022-03-18 01:27:21 UTC
- 2022-03-18 01:24:54 UTC
- 2022-03-18 01:23:16 UTC
- 2022-03-18 01:23:13 UTC
- 2022-03-18 01:44:38 UTC
- 2022-03-18 01:40:38 UTC
- 2022-03-18 01:37:36 UTC
- 2022-03-18 02:29:50 UTC
- 2022-03-18 03:12:11 UTC
- 2022-03-18 03:12:07 UTC
- 2022-03-18 03:02:06 UTC

- 2022-03-18 03:01:47 UTC
- 2022-03-18 03:16:02 UTC
- 2022-03-18 03:54:39 UTC
- 2022-03-18 03:54:38 UTC
- 2022-03-18 03:54:33 UTC
- 2022-03-18 03:54:28 UTC
- 2022-03-18 03:52:07 UTC
- 2022-03-18 03:52:02 UTC
- 2022-03-18 03:51:55 UTC
- 2022-03-18 03:48:57 UTC
- 2022-03-18 03:48:41 UTC
- 2022-03-18 03:48:17 UTC
- 2022-03-18 03:48:13 UTC
- 2022-03-18 03:48:10 UTC
- 2022-03-18 03:47:59 UTC
- 2022-03-18 04:31:33 UTC
- 2022-03-18 07:08:21 UTC
- 2022-03-18 07:07:56 UTC
- 2022-03-18 07:07:52 UTC
- 2022-03-18 07:01:18 UTC
- 2022-03-18 07:01:13 UTC
- 2022-03-18 08:14:02 UTC
- 2022-03-18 08:13:45 UTC

- 2022-03-18 08:33:13 UTC
- 2022-03-18 08:23:34 UTC
- 2022-03-18 09:18:22 UTC
- 2022-03-18 09:18:13 UTC
- 2022-03-18 09:18:05 UTC
- 2022-03-18 09:17:59 UTC
- 2022-03-18 09:17:52 UTC
- 2022-03-18 09:36:50 UTC
- 2022-03-18 10:58:31 UTC
- 2022-03-18 10:53:42 UTC
- 2022-03-18 10:53:39 UTC
- 2022-03-18 10:53:36 UTC
- 2022-03-18 10:53:34 UTC
- 2022-03-18 10:53:22 UTC
- 2022-03-18 10:43:40 UTC
- 2022-03-18 11:11:43 UTC
- 2022-03-18 11:47:13 UTC
- 2022-03-18 11:53:29 UTC
- 2022-03-18 11:52:21 UTC
- 2022-03-18 12:17:27 UTC
- 2022-03-18 12:09:25 UTC
- 2022-03-18 13:19:15 UTC
- 2022-03-18 13:19:10 UTC

- 2022-03-18 13:19:09 UTC
- 2022-03-18 13:19:03 UTC
- 2022-03-18 14:38:43 UTC
- 2022-03-18 14:38:28 UTC
- 2022-03-18 15:35:48 UTC
- 2022-03-18 16:46:46 UTC
- 2022-03-18 16:45:35 UTC
- 2022-03-18 17:55:15 UTC

(referred to herein and in Attachment B as "the Target Cell Phone"), that is in the custody or control of **T-Mobile US, Inc.** (referred to herein and in Attachment B as the "Service Provider"), a wireless communications service provider that is headquartered at 4 Sylvan, Parsippany, NJ 07054.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Service Provider, including any information that has been deleted but is still available to the Service Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Service Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

a. The following subscriber and historical information about the customers or subscribers associated with the Target Cell Phone for the time period of March 1, 2022, to the date of this warrant's execution:

i. Names (including subscriber names, user names, and screen names);

ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

iii. Local and long distance telephone connection records;

iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

v. Length of service (including start date) and types of service utilized;

vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Target Cell Phone, including:

(A) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

(ii) information regarding the cell tower and antenna face (also known as "sectors" through which the communications were sent and received) as well as per-call measurement data (also known as "real-time tool" or "RTT")].

b. Information associated with each communication to and from the Target Cell Phone for a period of 30 days from the date of this warrant, including:

i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;

ii. Source and destination telephone numbers;

iii. Date, time, and duration of communication; and

iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which the Target Cell Phone will connect at the beginning and end of each communication as well as per-call measurement data (also known as "real-time tool" or "RTT").

The Court has also issued an order pursuant to 18 U.S.C. § 3123, for such information associated with the Target Cell Phone.

c. Information about the location of the Target Cell Phone for a period of 30 days, during all times of day and night. "Information about the location of the Target Phone" includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information.

i. To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of the Service Provider, the Service Provider is required to disclose the Location Information to the government. In addition, the Service Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the

Service Provider's services, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

ii. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

II. Information to be Seized by the Government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Hobbs Act Robbery, 18 U.S.C. § 1951(a), Brandishing a Firearm During a Crime of Violence, 18 U.S.C. § 924(c), of Felon in Possession of a Firearm, in, 18 U.S.C. §§ 922(g)(1) and 924(a)(2). An arrest warrant was issued the same day for Antonio D. MOORE (DOB XX/XX/1992) including, but not limited to, information pertaining to the following matters:

(a) MOORE's location(s)

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Service Provider in order to locate the things particularly described in this Warrant.